



POST WEBINAR REPORT

# NERO Cybersecurity Training Series

Empowering SMEs with Practical  
Skills to Detect, Respond, and  
Defend Against Cyber Threats

Hands-On Cybersecurity Training Series

26 November 2025 | 3 December 2025 | 19 January 2026



Funded by  
the European Union



**ECCC**  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE

# Executive Summary

The **NERO Hands-On Cybersecurity Training Series**, held from 26 November 2025 to 19 January 2026, provided small and medium-sized enterprises (SMEs) across Europe with a practical and engaging approach to strengthening their cybersecurity defences. The series consisted of three interactive online webinars, each featuring three expert-led modules that combined insights, hands-on exercises, and open discussions, enabling participants to apply the skills they learned within their organisations.

The first webinar, [Building Cybersecurity Awareness and Defence Foundations for SMEs](#), introduced participants to cybersecurity fundamentals, cyber incident and risk handling, and social engineering techniques, providing a strong foundation for understanding and mitigating basic cyber threats. The second webinar, [Advanced Threat Detection and Privacy Protection for SMEs](#), focused on advanced network security, software security, and intrusion detection systems, equipping participants with practical strategies to protect their digital assets and sensitive data. The third and final webinar, [Immersive and Gamified Cybersecurity Practices for SMEs](#), offered hands-on exercises in privacy protection, incident response using CACAO Playbooks, cyber ranges training with an anti-phishing focus, and gamification-based cybersecurity training, allowing participants to consolidate their skills through interactive and immersive learning experiences.

Aligned with the [European Cybersecurity Skills Framework \(ECSF\)](#), the training series focuses on developing a shared understanding of cybersecurity roles and competencies and fostering collaboration within Europe's cybersecurity skills ecosystem. The series combines expert knowledge, real-world exercises, and interactive learning to explore cybersecurity concepts and practices, providing SMEs across Europe with opportunities to engage with strategies for strengthening resilience against evolving cyber threats.



# The Training Session

The **NERO Training Session Series** is a free, three-part, hands-on cybersecurity training designed for European SMEs, running from 26 November 2025 to 19 January 2026. Each session delivers **three interactive training modules** combining expert insights, practical exercises, and interactive discussions, offering participants actionable skills to strengthen their organisations' cybersecurity defences through three focused training modules per session. SMEs across Europe are invited to take part in this engaging and practical learning experience, helping businesses protect themselves against ever-evolving cyber threats.

**What makes this training essential:** Reading about a cyber threat is one thing—responding to it in real time is a completely different skillset. This series gives participants the space to experiment, make mistakes, learn quickly, and walk away with sharper instincts, better tools, and a clearer understanding of their role in keeping systems safe.



**Training Session 1 – Building Cybersecurity Awareness and Defence Foundations** introduced SMEs to core cybersecurity concepts, incident handling, and social engineering threats, emphasising practical skills, regulatory compliance, and employee awareness.



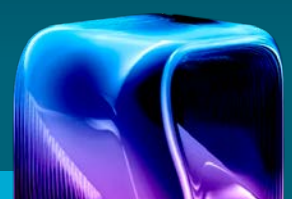
**Training Session 2 – Advanced Threat Detection and Privacy Protection** taught SMEs practical strategies for network security, penetration testing, advanced software protection with Snyc, and AI-enhanced intrusion detection using NIDS.



**Training Session 3 – Immersive and Gamified Cybersecurity Practices** provided SMEs with hands-on training through gamified cyber ranges for anti-phishing, scenario-based simulations via the KIOKU platform, and automated incident response using CACAO playbooks on the Sphinx platform.

Cybersecurity is both technical and human-centred. SMEs benefit from awareness, training, and practical tools. Gamification, scenario-based training, and automation enhance learning and resilience. Regulatory compliance, risk mitigation, and proactive defence are essential for business continuity.

Participants gain practical skills to recognise and respond to cyber threats, hands-on experience with cybersecurity tools and platforms, awareness of SME-specific risks and regulatory requirements, and exposure to gamified and scenario-based training for real-world readiness.



# Speakers

Charalambos Klitis, PhD, R&D Project Manager, [eBOS](#) (CY)

Introduced core cybersecurity concepts, including the CIA Triad, defence in depth, human factors, authentication, EU regulations (GDPR, NIS2), and common threats. Emphasised awareness, strong passwords, and multi-factor authentication.



Davide Ariu – Co-founder & CEO, [Pluribus One](#) (IT)

Covered incident handling fundamentals, including preparation, detection, containment, eradication, and post-incident review. Highlighted regulatory requirements and the use of SOC tools and open-source frameworks for effective incident response.



Dimitris Koutras – Computer Science Teacher, [University of Piraeus Research Centre](#) (GR)

Focused on social engineering threats and human-centred attacks. Demonstrated practical training tools for phishing awareness, password testing, and interactive exercises to enhance employee vigilance.



Eleni Seralidou – Project Manager, [trustilio](#) (NL)

Presented advanced software security practices using Snyk, covering code, dependencies, containers, and infrastructure-as-code scanning, highlighting automation, prioritisation, and privacy risk mitigation.



Dimitris Asimopoulos – Electrical & Computer Engineer/AI Engineer, [MetaMind Innovations](#) (GR)

Introduced Network Intrusion Detection Systems (NIDS), deployment strategies, signature vs anomaly detection, and AI/ML integration for improved detection of modern cyber threats.



Wissam Mallouli (Montimage) – Senior Researcher and CTO, [Montimage](#) (FR)

In the 2nd training session, he covered network security essentials and SME-focused penetration testing strategies, including vulnerability scanning, network segmentation, monitoring, and hands-on pen-testing tools. In the 3rd session, he demonstrated cyber range training for anti-phishing, offering a safe, gamified environment to practice detecting and responding to phishing attacks.



Ole Höfener – Project Manager, [Massive Dynamic Sweden](#) (SE)

Demonstrated scenario-based cybersecurity training with the KIOKU platform, allowing participants to navigate realistic attack simulations and learn decision-making under pressure.



Kostas Poullos – Senior Manager, [Sphynx Greece](#) (GR)

Introduced automated incident response with CACAO playbooks via the Sphinx platform, showing how structured, executable workflows improve efficiency, interoperability, and operational consistency in incident handling.





# Session Summaries & Learning Modules

This section outlines the structure and key learning outcomes of each webinar within the series. Organised across three progressive sessions and nine specialised modules, the programme guides participants from foundational cybersecurity concepts to advanced technical practices and immersive, scenario-based training.

Each module builds practical competence, strengthens risk awareness, and supports SMEs in developing structured, sustainable cybersecurity capabilities tailored to today's evolving digital threat landscape.

## Session 1: Building Cybersecurity Awareness and Defence Foundations for SMEs

On 26 November 2025, the first training session of the series on “[Building Cybersecurity Awareness and Defence Foundations](#)” offered SMEs a comprehensive introduction to cybersecurity. Charalambos Klitis (eBOS) covered core concepts, human factors, authentication, EU regulations, and common threats, emphasising awareness and strong security practices. Davide Ariu (Pluribus One) explained incident handling fundamentals—including preparation, detection, containment, and post-incident review—highlighting regulatory compliance and practical SOC tools. Dimitris Koutras (UPRC) focused on social engineering and human-centred attacks, demonstrating phishing awareness, password testing, and interactive exercises to enhance employee vigilance.

The event attracted 60 registrants, with 32 participants from 19 countries (15 EU, 4 Non-EU), representing a 53% attendance rate and strong international engagement.



## Module 1: Cybersecurity Fundamentals – Charalambos Klitis (eBOS)

This module introduced SMEs to cybersecurity essentials, emphasising the protection of digital systems—computers, mobile devices, servers, and cloud infrastructure—from threats such as hackers, cybercriminals, and state actors. Core concepts included the CIA Triad (Confidentiality, Integrity, Availability), Defence in Depth, and Zero Trust principles, with particular attention to mitigating human errors. Participants were also introduced to EU regulations such as GDPR and NIS2, standards such as ISO 27001, and common threats including phishing, ransomware, malware, supply chain attacks, and AI-driven exploits.

### Key Learnings:

Maintain awareness, adopt strong passwords and multi-factor authentication (MFA), follow Zero Trust principles, update systems regularly, and select security tools strategically. Awareness, layered defences, and regulatory compliance form the foundation of cybersecurity.

### Real-World Relevance for SMEs:

For SMEs with limited IT resources, foundational security practices are often the difference between resilience and business disruption. A single ransomware attack or data breach can lead to financial loss, regulatory fines, reputational damage, or even business closure. Implementing layered defences, MFA, regular updates, and compliance with EU regulations helps SMEs reduce exposure, maintain customer trust, and ensure operational continuity.

## Module 2: Cyber Incident and Risk Handling Fundamentals – Davide Ariu (Pluribus One)

This module covered the full lifecycle of incident response, from preparation and detection to containment, eradication, recovery, and post-incident review. Participants learned how to identify critical assets, monitor systems for threats, mitigate damage effectively, and align response practices with regulatory requirements, including the Cyber Solidarity Act, NIS2 Directive, and Cyber Resilience Act. Emerging threats—including automated attacks, supply chain compromises, web application vulnerabilities, and AI-layer attacks—were discussed alongside practical response tools such as Endpoint Detection & Response (EDR), Network Detection & Response (NDR), TheHive, Cortex, MISP, and Velociraptor.

### Key Learnings:

Develop and test incident response plans, clearly define roles and communication flows, implement continuous monitoring, and proactively improve response capabilities. Structured preparation significantly reduces cyber incident impact.

### Real-World Relevance for SMEs:

SMEs often lack dedicated security teams, making structured preparation critical. Without a clear response plan, even minor incidents can escalate into costly crises. Defining responsibilities, testing procedures, and ensuring regulatory compliance enable SMEs to respond quickly, minimise downtime, limit financial losses, and demonstrate accountability to customers and authorities.

## Module 3: Social Engineering & Human-Centred Cyber Threats – Dimitris Koutras (UPRC)

This module highlighted the human-factor dimension of cybersecurity, demonstrating how attackers exploit psychology rather than technical vulnerabilities. Techniques such as phishing, smishing, vishing, pretexting, and physical impersonation were examined, alongside psychological triggers including authority, urgency, fear, curiosity, and familiarity. Real-world cases illustrated the significant financial and operational damage



caused by social engineering. Practical demonstrations using NERO platform tools enabled participants to practice phishing detection, test password strength, and engage in interactive training scenarios.

**Key Learnings:**

Increase employee awareness, conduct regular training, verify sensitive requests independently, enforce strong password and MFA policies, and implement practical simulation exercises. Social engineering succeeds through human manipulation; vigilance and training are the most effective defences.

**Real-World Relevance for SMEs:**

Because SMEs rely heavily on trust-based communication and often operate with lean teams, employees are prime targets for phishing and impersonation attacks. A single fraudulent invoice, compromised email account, or stolen credential can result in substantial financial and reputational damage. Investing in regular awareness training and verification procedures empowers staff to act as the first line of defence and significantly reduces the risk of successful attacks.



## Session 2 – Advanced Threat Detection and Privacy Protection

The second training session, held on 3 December 2025, focused on “[Advanced Threat Detection and Privacy Protection for SMEs](#).” The session explored network security fundamentals, penetration testing methodologies, advanced software security practices, and intrusion detection systems (IDS). Participants gained practical, SME-oriented strategies for strengthening their security posture, including automated vulnerability management using Snyk and the deployment of AI-enhanced Network Intrusion Detection Systems (NIDS) to identify and respond to modern cyber threats.

The event recorded 43 registrations, with 30 active participants, representing 18 countries (15 EU and 3 non-EU). With an attendance rate of approximately 70%, the session demonstrated strong international interest and engagement across the SME community.

# NERO

Hands-On Cybersecurity Training Series

### Advanced Threat Detection and Privacy Protection for SMEs

**3 December 2025**

10:00–11:30 CET



Funded by  
the European Union



ECCE  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE



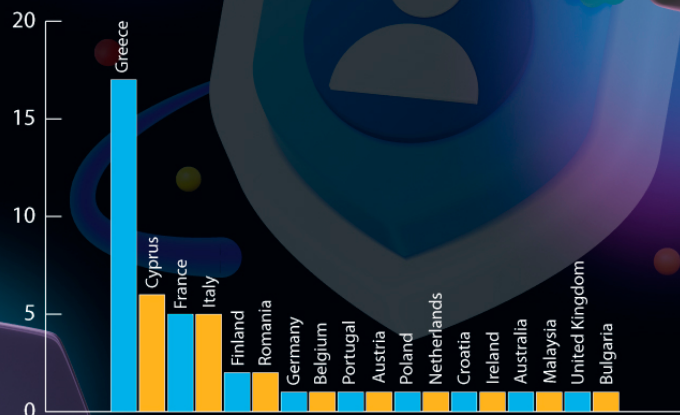
**43 Registrants**



**30 Participants**



**18 countries: 15 EU and 3 Non-EU**



## Module 4: Network Security Essentials & Penetration Testing – Wissam Mallouli (Montimage)

This module introduced SMEs to network security fundamentals and penetration testing as a proactive defense strategy. Participants learned that even a single vulnerable device can compromise an entire network and that common weaknesses include outdated firmware, weak passwords, flat network designs, and lack of monitoring. Best practices covered network segmentation, least privilege access, continuous monitoring, regular patching, and preparation of recovery and incident response plans. Penetration testing methodology—from reconnaissance to exploitation and post-exploitation analysis—was explained with practical tools such as Nmap, OpenVAS, and Metasploit, emphasising ethical hacking to discover vulnerabilities before attackers do.





### Key Learnings:

- Network security is a business enabler; proactive testing builds resilience.
- Segment networks and apply least privilege to limit risk.
- Regular penetration testing is essential for prevention and regulatory compliance.
- Practical, SME-focused tools enable effective, low-cost network protection.

### Real-World Relevance for SMEs:

SMEs often operate with limited IT staff and mixed legacy systems. Even a single weak device or poorly configured network can allow attackers to move laterally and compromise sensitive data, disrupt operations, or damage reputation. By segmenting networks, enforcing least privilege, and performing regular penetration tests, SMEs can identify vulnerabilities early, reduce exposure, and maintain operational continuity without large security budgets.

## Module 5: Software Security – Eleni Seralidou (trustilio)

This module focused on advanced software security for SMEs, demonstrating how tools like Snyk can detect, prioritise, and remediate vulnerabilities in code, dependencies, containers, and infrastructure-as-code (IaC). Participants learned to focus on vulnerabilities that are exploitable, secure containers, scan IaC for misconfigurations and privacy risks, and automate security policies to reduce operational overhead.

### Key Learnings:

- Focus on actionable vulnerabilities that attackers can realistically exploit.
- Harden containers and IaC early to prevent high-impact security and privacy risks.
- Automation ensures continuous security without slowing development.
- SMEs can achieve strong security with cost-effective, practical tools integrated into developer workflows.

### Real-World Relevance for SMEs:

Many SMEs rely on third-party software, cloud platforms, and containerised applications. Unpatched dependencies or misconfigured IaC can expose sensitive business data or cause service disruptions. By prioritising actionable vulnerabilities, hardening containers, and integrating automated tools into development workflows, SMEs can maintain robust software security efficiently, ensuring compliance, protecting customer data, and reducing operational risk.

## Module 6: Intrusion Detection Systems (IDS) – Dimitris Asimopoulos (Metamind Innovations)

This module explained the fundamentals, deployment, and AI-enhanced capabilities of Network Intrusion Detection Systems (NIDS). Participants learned how NIDS monitor network traffic to detect suspicious activity, including DoS, port scanning, SQL injection, XSS, MITM attacks, ARP spoofing, and brute-force attempts. Detection methods—signature-based, anomaly-based, and hybrid—were covered, along with deployment strategies for critical subnets and high-value assets. AI and machine learning were highlighted to improve the detection of zero-day and evolving attacks. Open-source tools like Snort, Suricata, and Zeek were presented, showing that strategic placement and integration into incident response are essential for effectiveness.



### **Key Learnings:**

- ⌘ NIDS provide visibility and early detection, but do not prevent attacks; prevention requires layered security.
- ⌘ Strategic deployment and integration into incident response maximise effectiveness.
- ⌘ AI and ML enhance the detection of unknown threats and reduce false positives.
- ⌘ Combining monitoring, prevention, policies, and awareness creates robust SME security resilience.

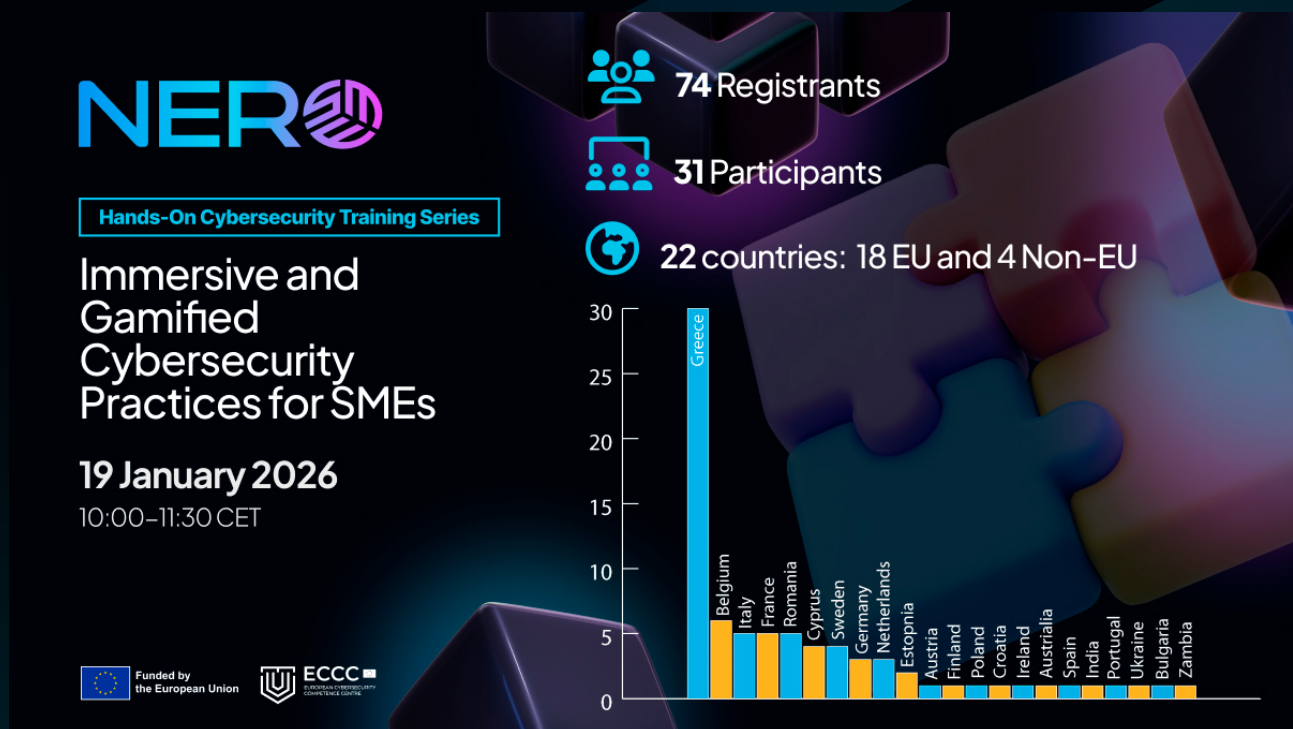
### **Real-World Relevance for SMEs:**

SMEs often lack full-time security monitoring, making early threat detection critical to avoid operational disruption. NIDS allow SMEs to detect suspicious activity in real time and respond before attacks escalate. When deployed strategically and integrated with incident response plans, NIDS combined with AI/ML capabilities help SMEs detect emerging threats, improve network visibility, and strengthen overall cybersecurity resilience without requiring large security teams.

## Session 3 – Immersive and Gamified Cybersecurity Practices

The third and final session of the three-part series, held on **19 January 2026**, focused on **“Immersive and Gamified Cybersecurity Practices for SMEs.”** It introduced hands-on training approaches, including gamified cyber-range anti-phishing exercises, scenario-based attack simulations via the KIOKU platform, and automated incident response using CACAO playbooks on the Sphinx platform, all of which emphasise decision-making, automation, and operational efficiency.

The session gathered 74 registrants, with 32 participants from 22 countries (18 EU, 3 non-EU), reflecting strong international engagement.



### Module 7: Privacy and Protection Enhancing Techniques, Incident Response Using CACAO Playbooks – Kostas Poullos (SPHYNX)

This module demonstrated how SMEs can transform traditional incident response procedures into structured, automated, and executable workflows using CACAO playbooks and the Sphinx platform. Participants learned the structure of CACAO playbooks (metadata, workflow logic, execution context) and how to design, execute, and monitor workflows in real time, integrating automation while keeping human oversight.

#### Key Learnings:

- ❏ CACAO standardises incident response playbooks into machine-readable, executable formats.
- ❏ Automation improves repeatability, consistency, and operational efficiency.
- ❏ Human-in-the-loop decision points can coexist with automated workflows.

☞ Sphinx platform enables design, validation, execution, and monitoring of playbooks.

#### **Real-World Relevance for SMEs:**

SMEs often lack large security teams, so automating incident response ensures rapid, consistent reactions to threats. Executable playbooks help SMEs respond to attacks efficiently, maintain compliance, reduce human error, and protect sensitive data without needing extensive resources.

### **Module 8: Cyber Ranges Training and Exercises (Anti-Phishing Focus) – Wissam Mallouli (Montimage)**

This session focused on gamified cyber range exercises to detect and respond to phishing attacks. Participants practiced identifying suspicious emails across progressive difficulty levels, using a platform simulating realistic attack scenarios without risking production systems. The module emphasised the rising threat of AI-generated phishing and the importance of combining people, process, and technology for defence.

#### **Key Learnings:**

- ☞ Phishing is the leading cyber threat to SMEs, increasingly sophisticated due to AI.
- ☞ Cyber ranges provide a safe, realistic environment for hands-on training.
- ☞ Gamification enhances engagement, learning retention, and practical skills.
- ☞ Effective defence combines awareness, policies, and technical safeguards (MFA, email filtering).

#### **Real-World Relevance for SMEs:**

Phishing is the most common cause of credential theft, ransomware, and business email compromise for SMEs. Practical exercises using cyber ranges help employees recognise attacks, improve decision-making, and reduce the likelihood of costly breaches, even in organisations with limited cybersecurity budgets.

### **Module 9: Gamification-Based Cybersecurity – Ole Höfener (Massive Dynamic Sweden)**

This module introduced scenario-based, interactive cybersecurity training using the KIOKU platform. Participants engaged in branching simulations where decisions affected the outcome of realistic cyber incidents, such as ransomware attacks. The training improved critical thinking, decision-making under pressure, and incident response skills.

#### **Key Learnings:**

- ☞ Scenario-based training enhances real-world incident response capabilities.
- ☞ Decision-tree simulations allow learners to experience cause-and-effect relationships.
- ☞ Immersive, hands-on exercises are more effective than theoretical training.
- ☞ Sector-specific scenarios make training relevant and practical for SMEs.

#### **Real-World Relevance for SMEs:**

SMEs face evolving cyber threats but often lack practical experience in handling incidents. Scenario-based training enables staff to practice responses safely, build confidence, and improve strategic thinking, reducing operational impact during real attacks.



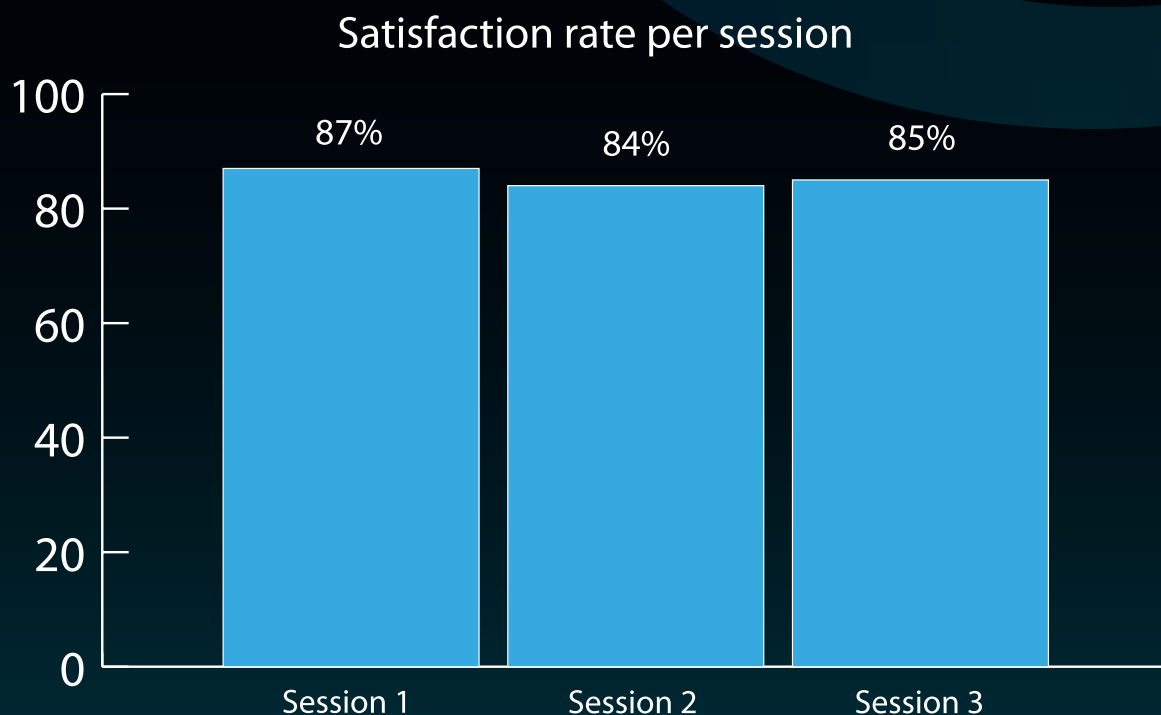


# Participant Insights & Feedback

This section presents a summary of participant feedback and engagement during the session, including key survey results, highlights from audience interaction, and notable questions raised. These insights provide valuable perspectives on the overall experience, relevance of the content, and areas of interest identified by participants.

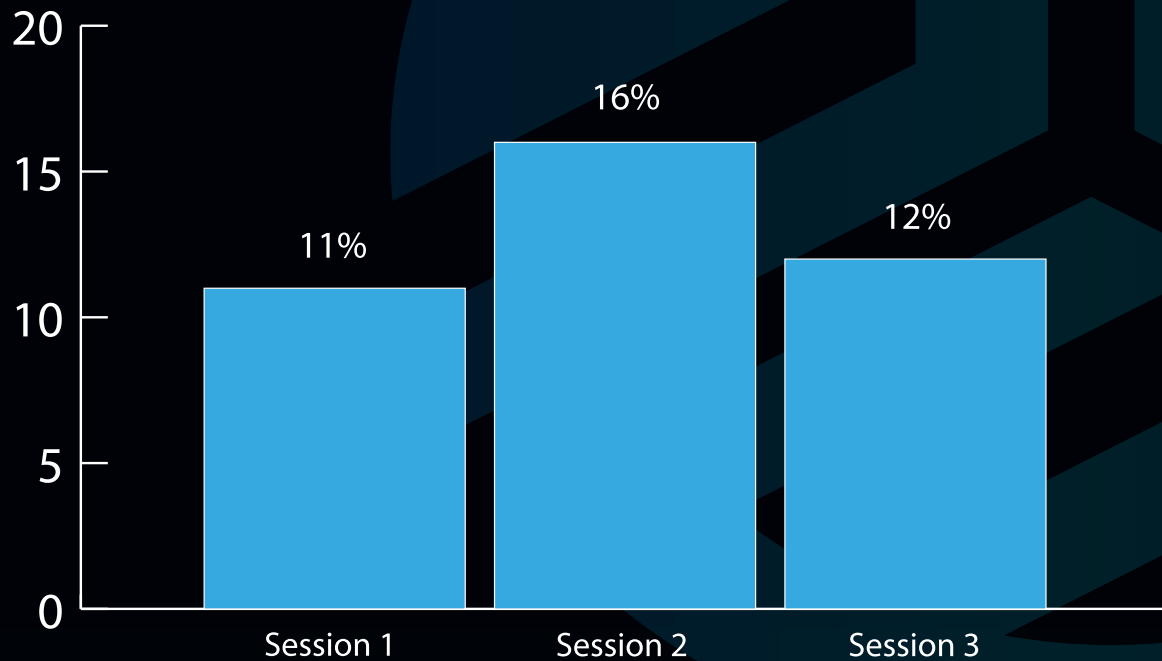
## Survey Results

As with all NERO training sessions, pre- and post-training questionnaires were administered to gather feedback and assess behavioural changes. Notably, this webinar series introduced a novel approach by incorporating some questions originally included in the pre-training survey during the sign-up process. This modification facilitated a more seamless flow throughout the session.



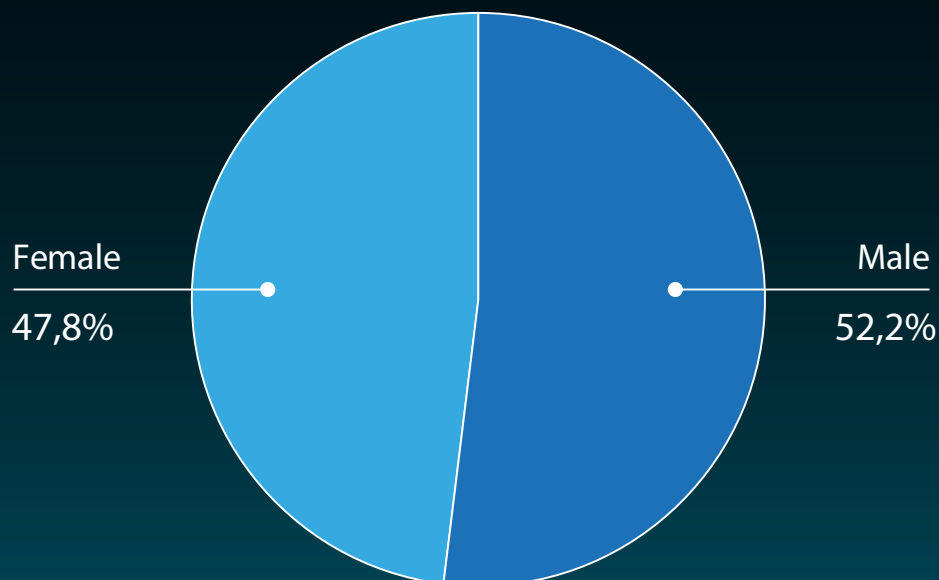
Satisfaction was measured using multiple five-point Likert scale questions. The results show constant satisfaction rates above 80% across all three webinars. With this result, they reach the NERO target of 80%.

## Increase in Participants' Cybersecurity Awareness & Hygiene



Next to satisfaction, participants' increase in cybersecurity awareness and cyber hygiene compared to before the training is measured as well. This measurement is based on quizzes that are part of both the pre- and post-training questionnaires and a self-assessment. The results show that all three sessions increased participants' awareness and cyber hygiene more than 10% on average. This highlights the effectiveness of the lectures.

## Participant Gender Distribution



Moreover, the NERO training webinar series could reach a highly diverse audience. Next to large number of nationalities that participated in the training lectures as shown further above, the graph above shows a near equal split in gender distribution.

# Q&A Highlights & Takeaways

Through its Hands-On Cybersecurity Training Series (2025–2026), NERO delivered practical, expert-led sessions covering foundational security, advanced threat detection, and immersive, gamified incident response training.

The following Q&A takeaways summarise the key insights, recurring questions, and practical recommendations shared throughout the webinar series.

## Webinar 1 | 26 November 2025

### Building Cybersecurity Awareness & Defense Foundations for SMEs

#### Q1: Is there one recommended password manager for SMEs?

**Answered by:** Charalambos Klitis (eBOS Technologies)

##### **Takeaway:**

There is no universally recommended password manager. Organisations should select tools based on:

- ▣ Company policies
- ▣ Budget
- ▣ Integration needs
- ▣ Security requirements

NERO is developing a cybersecurity marketplace that will include EU-based open-source and commercial tools with guidance for SMEs.

#### Q2: What is the most critical weakness in SME cybersecurity?

**Answered by:** Charalambos Klitis (eBOS Technologies)

##### **Takeaway:**

The human factor is the weakest link. Most successful attacks exploit:

- ▣ Weak passwords
- ▣ Phishing susceptibility
- ▣ Lack of awareness

Technical controls alone are insufficient without continuous employee training.



### Q3: How should SMEs approach compliance with EU cybersecurity regulations?

**Answered by:** Charalambos Klitis (eBOS Technologies)

#### **Takeaway:**

SMEs must understand and prepare for regulations such as:

- ▣ General Data Protection Regulation (GDPR) – Data protection and breach notification.
- ▣ NIS2 Directive – Risk management, incident reporting, and management accountability.
- ▣ Cyber Resilience Act – Security requirements for digital products.

Preparation includes incident response planning, documentation, and management-level accountability.

### Q4: Are standards like ISO 27001 enough to guarantee security?

**Answered by:** Charalambos Klitis (eBOS Technologies)

#### **Takeaway:**

No certification guarantees complete security. Standards such as ISO 27001 provide a structured framework and best practices for managing information security risks, but they do not eliminate threats. Effective cybersecurity requires continuous risk assessment, active monitoring, regular updates, employee awareness, and ongoing adaptation to evolving threats.

## Webinar 2 | 3 December 2025 Advanced Threat Detection & Privacy Protection for SMEs

### Q1: Why should SMEs perform penetration testing?

**Answered by:** Wissam Mallouli (Montimage)

#### **Takeaway:**

Penetration testing allows SMEs to identify vulnerabilities before attackers do. It improves resilience, supports compliance requirements, and ensures that security controls are functioning properly. Regular testing is essential due to evolving threats and infrastructure changes.

### Q2: Are open-source tools sufficient for SMEs?

**Answered by:** Davide Ariu (Pluribus One) & Dimitris Asimopoulos (Metamind Innovations)

#### **Takeaway:**

Yes, when strategically selected and properly managed. Examples discussed include:

- ▣ OpenVAS (vulnerability scanning)
- ▣ Snort / Suricata (IDS)
- ▣ TheHive (incident response management)

However, effectiveness depends on proper configuration, monitoring, and staff expertise. A well-managed, simple solution is often better than a complex system that cannot be maintained.



### Q3: How can SMEs prioritise vulnerabilities effectively?

**Answered by:** Eleni Seralidou (Trustilio)

#### **Takeaway:**

SMEs should prioritise vulnerabilities based on:

- 🔲 Exploit maturity
- 🔲 Real-world exploitability
- 🔲 Business impact
- 🔲 Fix availability

Rather than focusing solely on CVSS scores, organisations should concentrate on vulnerabilities that attackers are actively exploiting and that pose immediate risk.

Not all CVEs require immediate action. Focus on exploitable and high-impact risks first.

### Q4: Do Intrusion Detection Systems (NIDS) replace firewalls?

**Answered by:** Dimitris Asimopoulos (Metamind Innovations)

#### **Takeaway:**

No. Firewalls filter traffic; NIDS monitor and analyse behaviour.

Security must be layered:

- 🔲 Firewalls
- 🔲 IDS/NIDS
- 🔲 Monitoring systems
- 🔲 Incident response plans

AI-enhanced NIDS improve detection of zero-day and anomalous threats but do not eliminate the need for traditional controls.

### Q5: Is AI replacing traditional cybersecurity systems?

**Answered by:** Dimitris Asimopoulos (Metamind Innovations)

#### **Takeaway:**

AI is not replacing traditional cybersecurity systems; it is strengthening them. AI-driven detection enhances the ability to identify anomalies, zero-day threats, and evolving attack patterns in real time. However, the most effective defence remains a hybrid approach—integrating signature-based tools, behavioural analytics, and human expertise within a layered security strategy.

## Webinar 3 | 19 January 2026

### Immersive & Gamified Cybersecurity Practices for SMEs

#### Q1: Why is phishing still the leading cyber threat?

**Answered by:** Wissam Mallouli (Montimage)

##### **Takeaway:**

Phishing targets human psychology—leveraging urgency, fear, authority, and curiosity—rather than technical vulnerabilities. According to the European Union Agency for Cybersecurity (ENISA):

- ▣ Nearly 60% of intrusions begin with phishing.
- ▣ Over 80% of AI-generated phishing emails are highly realistic and personalised.

Phishing succeeds because it exploits human behaviour, not technology.

#### Q2: How effective is gamified cybersecurity training?

**Answered by:** Wissam Mallouli (Montimage) & Ole Höfener (Massive Dynamic Sweden)

##### **Takeaway:**

Gamified and Cyber Range-Based Training:

- ▣ Enhances engagement and motivation
- ▣ Boosts knowledge retention
- ▣ Encourages participation through competition
- ▣ Builds behavioural memory and decision-making confidence

Cyber ranges provide a safe, realistic environment to simulate attacks, allowing participants to practice detecting phishing and responding to incidents without risking real systems, strengthening both practical skills and confidence.

#### Q3: What makes scenario-based training valuable?

**Answered by:** Ole Höfener (Massive Dynamic Sweden)

##### **Takeaway:**

Interactive decision-tree simulations:

- ▣ Improve critical thinking
- ▣ Simulate real-world pressure
- ▣ Teach consequence-based learning
- ▣ Strengthen incident response skills

Hands-on practice is significantly more effective than passive lectures.

#### Q4: What problem does CACAO solve in incident response?

**Answered by:** Kostas Poullos (SPHYNX)

##### **Takeaway:**

Traditional playbooks are static and non-executable.

CACAO:

- ▣ Standardises playbooks in a structured format

- ☐ Enables automation
- ☐ Supports interoperability
- ☐ Bridges documentation and execution

Automation improves repeatability, speed, and operational consistency.

## Trainers' Final Takeaways

- 💬 “Fundamental cybersecurity practices—combining technical safeguards, human awareness, and compliance with EU regulations—are essential for protecting digital assets and ensuring organisational resilience against evolving threats.” - Charalambos Klitis, eBOS
- 💬 “Preparation is critical—having a plan ensures organisations respond effectively without panic, reducing impact and improving resilience.” - Davide Ariu, Pluribus One
- 💬 “The most effective defence is awareness, training, and verification before trusting any request.” - Dimitris Koutras, UPRC
- 💬 “SMEs can strengthen cybersecurity by combining practical tools, proactive defences, and continuous testing - making security an integral part of business operations.” - Wissam Mallouli, Montimage
- 💬 “Designing secure software systems with limited resources requires careful planning during the development phase.” - Eleni Seralidou, trustilio
- 💬 “Strategically deployed NIDS, enhanced with AI and integrated into a layered security approach, give SMEs critical visibility and early threat detection to strengthen cybersecurity resilience.” - Dimitris Asimopoulos, MINDS
- 💬 “Gamified cyber range training equips SMEs to recognise, respond to, and mitigate AI-enhanced phishing attacks, making employees the first line of defence in strengthening organisational cybersecurity.” - Wissam Mallouli, Montimage
- 💬 “Scenario-based, hands-on training via the KIOKU platform enhances SMEs’ real-world cybersecurity decision-making by immersing participants in realistic, interactive attack scenarios.” - Ole Höfener, Massive Dynamic Sweden
- 💬 “Using CACAO playbooks with the Sphinx platform transforms incident response into standardised, executable workflows, enhancing automation, consistency, and operational efficiency while keeping human oversight where needed.” - Kostas Poullos (SPHYNX)

# Key Outcomes

This NERO training webinar series featured lectures from all modules of the NERO training curriculum. As a result, participants gained cybersecurity knowledge across a variety of topics such as social engineering, threat detection, and incident handling. Moreover, learners were guided through the sessions from a beginner level, covering cybersecurity basics to more advanced topics and hands-on exercises.

Furthermore, the NERO training curriculum is developed with the European Cybersecurity Skills Framework (ECSF) in mind, covering eleven of its twelve profiles.

## Recommendations & Next Steps

The NERO Project will continue to expand its cybersecurity training initiatives through both online webinars and in-person sessions. Future efforts will focus on targeting professionals in the healthcare, finance, and logistics sectors, aligning with the project's real-world use cases. Additionally, NERO will enhance its on-demand training resources, providing SMEs with flexible opportunities to strengthen their cybersecurity skills at their own pace.

The webinar series demonstrated that SMEs do not need large budgets to significantly improve their cybersecurity posture. What matters most is a combination of strategic planning, practical implementation, and continuous learning. Key elements for SMEs to achieve cybersecurity resilience include:

- 🗨️ **Structured Planning:** Define clear policies, risk assessments, and incident response strategies.
- 🗨️ **Employee Awareness:** Foster a security-conscious culture through regular training and simulations.
- 🗨️ **Practical Tools:** Select and implement cybersecurity solutions appropriate to the organisation's size, resources, and risk profile.
- 🗨️ **Strategic Prioritisation:** Focus efforts on the most critical assets and vulnerabilities.
- 🗨️ **Continuous Training:** Reinforce skills and awareness through repeated exercises and updates.
- 🗨️ **Incident Response Automation:** Streamline detection, reporting, and mitigation using tools and standards such as CACAO playbooks.

Cybersecurity maturity is an ongoing journey. Through its ecosystem, marketplace, training platforms, and practical guidance, the NERO Project empowers SMEs to turn awareness into measurable action, improving resilience, reducing risk, and supporting business continuity.



# About NERO

The NERO consortium is an EC-funded initiative (Grant Agreement No. 101127411) supported by the European Cybersecurity Competence Centre (ECCC). Its mission is to build stronger, more resilient digital ecosystems across Europe by empowering organisations — especially SMEs — to improve their cybersecurity capabilities.

Bringing together industry specialists, academic researchers, and technology experts, NERO delivers meaningful, hands-on learning experiences that translate complex cybersecurity challenges into actionable strategies. The consortium focuses on sectors such as healthcare, logistics, finance, and digital infrastructure, where awareness and preparedness are key to staying secure.

